TRINA A. HIGGINS, United States Attorney (#7349)
CHRISTOPHER BURTON, Assistant United States Attorney (NV #12940)
Attorneys for the United States of America
Office of the United States Attorney
20 North Main Street, Suite 208
St. George, Utah 84770
Telephone: (435) 634-4266
Christopher.Burton4@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A WARRANT AUTHORIZING THE SEARCH OF A PREMISES LOCATED AT 2028 W. 1600 N. SAINT GEORGE, UTAH, 84770	AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT **Under Seal** Case No. 4:24-mj-00022 PK
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A WARRANT AUTHORIZING THE SEARCH OF JOHNATHAN GOLDEN GUNTER, DOB [redacted]	AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT **Under Seal** Case No. 4:24-mj-00023 PK
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A WARRANT AUTHORIZING THE SEARCH OF APPLE IPHONE, BEARING IMEI 351461186630959	AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT **Under Seal** Case No. 4:24-mj-00024 PK

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

INTRODUCTION

I, Ivan Murray, a Special Agent (SA) with Homeland Security Investigations (HSI), assigned to the HSI St. George, Utah office, being duly sworn under oath, do hereby depose and state as follows:

1. I am a Special Agent with Homeland Security Investigations (HSI), Office of the Assistant Special Agent in Charge in Salt Lake City, Utah. I have been employed as a Special Agent with HSI beginning in 2011 and currently assigned to assist the Federal Bureau of Investigation's Child Exploitation Task Force (CETF) as well as the Utah Attorney General's Internet Crimes Against Children Task Force (ICAC). Prior to my current position with HSI, I was employed as a Criminal Investigator/Special Agent with Internal Revenue Service - Criminal Investigative Division for approximately seven years. I've received training in the area of child-pornography investigations and I've had the chance to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received additional training from CETF and ICAC relating to online, undercover chatting investigations (explained later), as well as peer-2-peer or P2P investigations. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. Specifically, I have participated in numerous investigations relating to the sexual exploitation of children over the Internet since 2013.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants

issued under the authority of the United States. I am charged with the investigation of criminal violations relating to child exploitation and child pornography including violations pertaining to the online enticement of a minor, as well as the production, distribution, receipt, and possession of child pornography in violation of Title 18 U.S.C. §§ 2422(b), 2251, 2252, and 2252A.

PURPOSE OF THE AFFIDAVIT

3. I submit this affidavit in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure. I make this affidavit to request a warrant to search the property located at 2028 W. 1600 N. Saint George, Utah 84770, further described in Attachment A-1 (the "SUBJECT PREMISES"), as well as any persons found at or on the premises at the time of the search, further described in Attachment A-2 (Johnathan Golden GUNTER) and electronic devices on his person or within his immediate reach, further described in Attachment A-3 ("SUBJECT DEVICE") for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B) (involving the transportation, receipt, distribution, and possession of child pornography) (the "Target Offenses"), as described in Attachment B.

4. This affidavit is being submitted for the limited purpose of securing a search warrant. As such, I have not included each and every known fact concerning this investigation. I have set forth only the facts I believe to be necessary to establish probable cause for the requested search warrant. The statements in this affidavit are based in part on information provided by law enforcement officers assigned to other

law enforcement agencies, other special agents, and employees of HSI, and my experience and background as a Special Agent of HSI.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B) have been committed by Johnathan GUNTER. There is probable cause to search the information described in Attachments A-1, A-2, and A-3, for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

APPLICABLE LAW

6. Title 18, U.S.C. § 2252A(a)(1) makes it a crime to knowingly mail, ship, or transport any child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

7. Title 18, United States Code, Sections 2252A(a)(2) and (b)(1) prohibit a person from knowingly receiving or distributing child pornography, or any material that contains child pornography, using any means or facility of interstate or foreign commerce or that has been mailed or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. Title 18, United States Code, Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or

transported in or affecting interstate or foreign commerce by any means, including by computer. The term "child pornography" is defined in 18 U.S.C. § 2256(8).

DEFINITIONS

9. The following definitions apply to this affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. "Electronic Service Providers" or "ESPs," as used herein, are telecommunications carriers, providers of electronic communication service, providers of

a remote computing service, any other communication service providers who have access to wire or electronic communications either as such communications are transmitted or as such communications are stored, or any officer, employee, or agent of an ESP.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. "Hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP

address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph

records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as flash drives, SD cards, floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), optical disks, printer buffers, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.

p. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. "Storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

10. Based on my training and experience in the investigation of computer-related crimes, I know the following:

a. Those individuals with a sexual interest in children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media. They often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. In the past, these materials commonly included hard copies material - that is, pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc. More recently, computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

d. Regardless of whether an individual stores their child pornography via hard copy or digital files, the material is typically stored in a location that is safe, secure,

private – and easily accessible. This is generally the person's home, in their vehicle, on their person, or in cloud-based online storage that can be easily accessed using devices in their home, in their vehicle, or on their person. This easy access is important to enable the individual to view the child pornography images often and in private.

e. Individuals who have a sexual interest in children or images of children typically retain their material - pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica- for many years. Child pornography images in particular are highly valued and are often maintained for several years. Such individuals prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

g. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as

"WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store tens or hundreds of thousands of high-resolution photographs or videos.

h. A device known as a modem allows any computer to connect to another computer using a telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally billions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

i. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, "thumb," "jump," or "flash" drives, and memory cards, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

j. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

k. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

l. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

m. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or

unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

n. Collectors and distributors of child pornography often use online resources to retrieve, share, and store child pornography. Non-pornographic, seemingly innocuous images of minors are often found in accounts that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

o. Further, the online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. The online storage accounts are often free but can involve a charge. A subscriber assigned a free online storage account frequently can set up such accounts by providing limited identifying information. Any information provided is frequently fictitious in an attempt to preserve the anonymity of the user. Consequently, even if it is known that a collector or distributor of child pornography is a

subscriber of a free online storage service, the service provider frequently will have no records in that subscriber's name. Instead, the online service will only be able to identify files, including child pornography, that are associated with a "login," or unique, user-created identity the subscriber uses to "log on" to the online service.

p. Such an online storage account is particularly useful to a collector or distributor of child pornography. Such a subscriber can collect, store, view and distribute electronic images, including child pornography, directly from the online service. Consequently, the illegal files have minimal contact with the subscriber's home computer. The subscriber can also manipulate the files on an online storage service from any computer connected to the Internet. Nonetheless, evidence of an online storage account is often found on a home computer of a user subscribing to such a service. Evidence of an online storage account may take the form of passwords located in encrypted, archived, or other files on the user's home computer. Other evidence can also be found through unique software that may exist on a user's home computer that has been developed by the online storage service. This unique software will frequently contain evidence not only of the existence of such accounts, but the login and password.

q. I know from training and experience that a person trading in, receiving, transporting, distributing, or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicates with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child sexual exploitation. Such offenders

rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

r. Digital evidence is not limited to computers. I have been involved in cases where persons engaged in the type of crime under investigation can access the Internet, display images reflecting their interests or participation in the crime and communicate with other individuals with the same interests using digital storage devices to include cellular telephones, email devices, and personal digital assistants. These devices are frequently found to contain chat communications in the form of short message service (SMS) messages as well as enabling Internet and digital cellular network access. In my training and experience, I have found these devices in residences and vehicles belonging to the perpetrator as well as on the person of suspect(s).

s. Even if an individual uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in their homes, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

t. Often, when a person uses a digital device to access, receive, possess, or distribute child pornography, other digital devices belonging to or used by that same perpetrator will likewise contain evidence of child pornography. This can be because the

perpetrator has used multiple devices to commit child pornography offenses, or because the perpetrator has "synced" their devices such that the content of one device is accessible on another device, or because the perpetrator has transferred all or a portion of their then-existing child pornography collection from one digital device to another.

u. I know from training and experience that the complete contents of digital devices or online accounts may be important to establishing the actual user who has dominion and control of an online account at a given time. Online accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. So, information stored in connection with an online account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation. This helps establish and prove each element of the crime or alternatively, may exclude the innocent from further suspicion. In my training and experience, an online user's account activity, IP log, location information, search history, stored electronic communications, and other data retained by providers, can indicate who has used or controlled an online account or can provide context for the crime under investigation. This can include evidence of motive and intent to commit a crime (e.g., communications about planning crimes), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date, and time) may be evidence of who used or controlled the account at a relevant time. Further, account activity, especially when paired with other evidence of

the crime, can show how and when the account was accessed or used, and may reflect a user's motive or state of mind when doing so. For example, as described herein, providers log the Internet Protocol (IP) address from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Especially when considered in context with other evidence, such information allows investigators to understand the geographic and chronological contest of an account's access, use, and events relating to the crime under investigation. Location data also helps with this. Providers allow users to "tag" their location in posts to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the account user or other suspects.

v. I know from training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or code words (which require entire strings or series of email conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images, and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an email or the manipulation and combination of keys on the computer keyboard to convey and idea, such as the use of a colon and parentheses ":)" to convey a smile or agreement) to discuss matters. Keyword searches would not account for any of these possibilities, so actual

review of the contents of an online account by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the account.

w. It is also possible to use pictures, images, and emoticons (images used to express an emotion or idea such as a happy face inserted into the content of an email or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parentheses ":)" to convey a smile or agreement) to discuss matters. Actual review of the contents of a photo-sharing account by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the account.

x. I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this affidavit and in Attachment B to prevent unnecessary invasion of privacy and overbroad searches. I have learned through practical experience that various emails often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between communication threads and contents of accounts, and any respective attachments, looking at one piece of

information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. Therefore, to obtain the full picture and meaning of the data from the information sought in Attachment B of this application, and to maintain its admissibility at trial, the Government needs to maintain access to all the resultant data. The completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As with all evidence, the Government will obtain the contents of the items in its custody and control, without alteration.

BACKGROUND ON SNAPCHAT

11. According to the Snap Inc. Law Enforcement Guide, Snapchat is a visual messaging app made by Snap Inc. ("Snap") that enhances relationships with friends, family, and the world. Snapchat empowers people to express themselves, live in the moment, learn about the world, and have fun together. Snapchat is available through the iPhone App Store and Google Play Store, while the web application can be accessed at web.snapchat.com.[1]

12. One of the principal features of Snapchat is that images and messages are *usually* only available for a short period of time before they become inaccessible to their recipients.

13. I know from experience that Snapchat is a popular social-media application that is sometimes used by individuals seeking to collect and distribute child pornography.

[1] Snap Inc. Law Enforcement Guide. Last updated August 15, 2023. www.snapchat.com/lawenforcement

Because of the vanishing nature of media being shared between and among its users, many users utilizing this platform for these nefarious purposes believe the application offers a high degree of anonymity from law enforcement.

THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

14. The National Center for Missing and Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit 501I(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited-child issues. To further their mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Program (CVIP). NCMEC makes information submitted to the CyberTipline and CVIP available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC performs its programs of work pursuant to its own private mission and independent business operations. NCMEC does not act in the capacity of or under the direction or control of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.

PROBABLE CAUSE

15. During July of 2023, NCMEC received an investigative lead (CyberTip Number 166881890) from social-media company, Snapchat. According to the lead, a

Snapchat user with a username of Tonythetigger83 (not the subject user of this investigation) uploaded six files of child pornography (aka "CSAM" or Child Sex Abuse Material) to his account. Based on geolocation information listed in the lead, CyberTip 166881890 was assigned to Watertown Police Department (located in South Dakota) for further review.

16. Det. Jeremy Bjerke of Watertown Police Department was tasked with evaluating CyberTip 166881890. In reviewing the lead, Det. Bjerke determined that Snapchat user Tonythetigger83 had in fact uploaded six files of child pornography to his account. I too reviewed these files and concur that all six files depicted child pornography. Det. Bjerke then sought to identify the user of the Snapchat account and took several actions towards this end. Among other things, Det. Bjerke secured a search warrant for the contents of the Snapchat account, Tonythetigger83. From the search warrant returns, Det. Bjerke determined that Snapchat user Tonythetigger83 had communicated and exchanged child pornography with another Snap user identified as "Thomas_evans977" (the subject user of this investigation).

17. In reviewing the files exchanged between these Snapchat users, records showed that on July 21, 2023, Thomas_evans977 sent an image to Tonythetigger83 of a minor-aged female, between the approximate ages of six and eight years, exposing her chest while only wearing red-colored underwear. Also on that date, Tonythetigger83 sent a file of child pornography to Thomas_evans977. The video file is one minute and 21 seconds in length and shows an adult male either vaginally raping or anally sodomizing a female who is approximately five years of age.

18. During October of 2023, Det. Bjerke secured a search warrant for the Thomas_evans977 account. Snapchat provided records including IP information for the account. Among other things, the records showed that on July 15, 2023, at 16:18:59 UTC, IP address 69.128.229.110 was utilized to access the Thomas_evans977 account. Further, Det. Bjerke was able to determine that this IP address was owned by TDS Broadband Service LLC ("TDS"). Det. Bjerke then issued a subpoena to TDS for subscriber records. On or about November 6, 2023, TDS provided subscriber data showing the IP address in question was assigned as follows on the date in time in question:

Bob Langnese
2028 W. 1600 N. Saint George, UT 84770 (SUBJECT ADDRESS)

19. A further review of the search warrant return for the Thomas_evans977 account revealed images ("selfies") of numerous male individuals who are believed to be potential owner(s)/operator(s) of the Snapchat account as well as likely residents of Washington County, Utah. Through facial-recognition technology, three individuals were identified from selfie images found in the account. These three individuals are identified as follows:

Cole Scott Rogers
2544 E. 2830 S. St. George, UT 84790 (Last known address)

Jade William Gunter
41 E. 600 S. Apt 41 St. George, UT 84770 (Last known address)

Johnathan Taylor Gunter
2696 E. 370 N. St. George, UT 84770 (Last known address)

20. The subscriber data for the Thomas_evans977 account showed that Thomas Roy Evans (hereafter, "Evans" – D.O.B. [redacted]) of Washington County, Utah is

potentially associated with the account as well. For instance, not only does Evans share the same name as the Snapchat username, but Evans' date of birth as listed in DMV records ([redacted]) is very close to the listed date of birth for the account ([redacted]). Through analysis of publicly available Facebook accounts, investigators learned that Evans is also associated with Jade William Gunter, who has selfie-style photos on the Thomas_evans977 account and the two appear to be stepbrothers. Other social-media associations between Evans and individuals bearing the last name of Gunter are numerous.

21. A review of the media contained in the Thomas_evans977 account revealed numerous files of CSAM. Listed below are the names and my descriptions of three CSAM files found in the account:

File Name: chat~media_v4~2023-07-21-16-21-34UTC~tonythetigger83~~saved~b~EiQSFW11UmU0V0Zna1VtSnBBejZOMEt1SxoAGgAyAX1IAlAEYAE~v4.mp4
File Description: The file is one minute in length and begins with two minor-aged children observed either partially or fully nude. One of the minor-aged females, approximately four years of age, is observed being orally sodomized (victim's mouth on an erect male penis). The minor's genitalia are briefly exposed to the camera lens. At the bottom of the screen is a possible darknet webpage address listed as "loliporn6s6edjjo.onion."

File Name: chat~media_v4~2023-07-21-16-21-34UTC~tonythetigger83~~saved~b~EiQSFTMzemxsbG9yUVFDaTVIMnk1MkNaeBoAGgAyAX1IAlAEYAE~v4.mp4
File Description: The video file is one minute and 20 seconds in length. The video begins with a still image showing the faces of a Hispanic male adult and a Hispanic female who is likely between the ages of four and six years of age. Later during the video, an adult male is observed either anally sodomizing or vaginally raping a female victim who approximates the same age as the female depicted in the still-image portion of the video.

File Name: chat~media_v4~2023-07-21-16-21-54UTC~tonythetigger83~~saved~b~EiQSFW5uU2t6U0RXYmVuMW5TRjFWYTZ0WRoAGgAyAX1IAlAEYAE~v4.mp4
File Description: This video file is one minute and 21 seconds in length. The video shows a minor-aged female child, approximately five years of age, being orally sodomized

(victim's mouth on a human male penis). The victim is seen wearing a tiger costume during the sexual abuse.

22. Text communications between the Thomas_evans977 account and Tonythetigger83 occurred on July 21, 2023, and were provided in connection with the records provided by Snapchat. As part of those communications, Tonythetigger83 asked Thomas_evans977 if he was in possession of images. Given the context and based on my experience, it is my opinion that the conversation between these two users was referencing sharing CSAM. In that context, Thomas_evans977 confirmed that he was in possession of both videos and images of child pornography. Thomas_evans977 also provided instruction to Tonythetigger83 as to how to use the Snapchat app to send CSAM.

23. As part of these communications, Snapchat records show that six files were then sent from the Thomas_evans977 account to the Tonythetigger83 account. A review of two of the files showed the images to be of prepubescent girls wearing panties and exposing their chests. Shortly thereafter, Tonythetigger83 sent three child pornography videos to Thomas_evans977 identical to the files described in ¶ 21 above.

24. Tonythetigger83 inquired of Thomas_evans977 as to whether he had ever engaged in sexual activity with minors. Thomas_evans977 confirmed that he had engaged in sexual activity with a minor who he stated was 10 years of age when the abuse started (it's unclear the current age of this victim). Thomas_evans977 further explained that the victim is friends with his sister. Thomas_evans977 also stated that he could possibly obtain "pics" of the victim. Given the context and based on my experience, it seems likely that Thomas_evans977 was explaining that he could produce child pornography with this same

unidentified victim. Thomas_evans977 shortly thereafter stated that his sister was 10 years of age and that he had engaged in sexual relations with her. From the communications provided, it's unclear to me whether Thomas_evans977 is referencing one or two victims. In reference to Thomas_evans977 and Tonythetigger83 potentially meeting one another to abuse the referenced victim(s), Thomas_evans977 stated that he is located in Washington.[2]

25. Because of the numerous potential individuals associated with the Thomas_evans977 account, I sought to identify the likely user of the account. In that effort, I observed that two Verizon IP addresses were utilized by the Thomas_evans977 account during July of 2023. I subsequently issued legal service to Verizon requesting subscriber data for the Verizon user utilizing these two IP addresses. In response, Verizon responded stating that no data could be produced for one of the IP addresses and that the other IP address is a "NATTING ROUTER IP" which prevented Verizon from providing subscriber records. However, Verizon did produce a spreadsheet listing all of the phone numbers utilizing this second IP address (along with assigned port numbers) for the period in question. From analyzing the spreadsheet, I was able to locate phone number (435) 599-0008, which was the same phone number listed in the records for the Thomas_evans977 account as being that account's *verified* phone number. I further learned that the phone number (435) 599-0008 was attributed to Verizon reseller, Tracfone.

26. Additional legal process was served to Tracfone to identify the subscriber of (435) 599-0008. In response, Tracfone provided records stating that the account was a

[2] Based on my training and experience as well as the investigation to date, I believe this is reference to Washington City or Washington County, both located in southern Utah.

prepaid account, and as such, no subscriber information was available; however, Tracfone provided a purchase receipt associated with the cell account dated January 25, 2024, wherein the customer listed was GUNTER. GUNTER's listed address on the receipt was listed at the SUBJECT ADDRESS (2028 W. 1600 N. Saint George, UT).

27. In response to a DHS summons issued to Tracfone, Tracfone provided records indicating that phone number (435) 599-0008 was changed to (435) 359-6851 on February 8, 2024. Tracfone also provided information stating that both phone numbers were utilizing an iPhone model 11S mobile device with an identical International Mobile Equipment Identity ("IMEI") number of 351461186630959 (SUBJECT DEVICE). I know from experience that an IMEI number is a unique device identifier.

28. During February of 2024, FBI personnel based in Salt Lake City, Utah, also assisted in this investigation and issued Subpoena Number 936498 to TDS Telecom for subscriber records relating to IP information associated with Thomas_evans977. Specifically, IP address 134.215.246.59 was utilize by Thomas_evans977 on July 23, 2023, at 23:58:33 UTC. The results of the subpoena revealed that the IP address was assigned to the following individual:

James Gunter
55 W. 700 S. Apt. 41 Saint George, UT 84770

29. Upon receiving these subscriber records from FBI personnel, I noted that TDS Telecom subscriber James Gunter shared the same last name as GUNTER. Through social-media and law-enforcement-database checks, I believe James Gunter to be the father of GUNTER. In my personal and investigative experience, it is common for individuals to

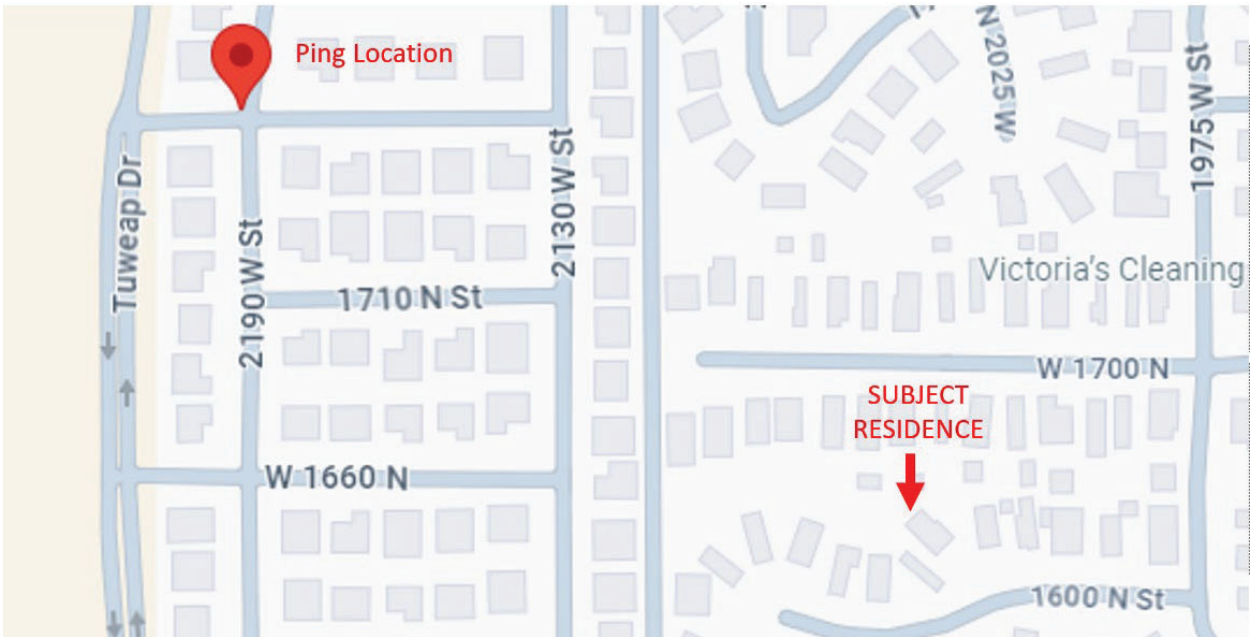
access the Internet via WiFi connections controlled by family members or friends when the individual visits the family's/friend's domicile.

30. During February of 2024, I contacted the United States Postal Service and inquired as to who was receiving mail at the SUBJECT PREMISES beginning in June of 2023. USPS stated the following individuals had or were receiving mail at this address:

Sally Lewis
Sally Langnese
Bob Langnese
Cody (no last name given)
Rissa Jean
Johnny Gunter
Dustin Cleveland
Marissa Langnese

31. I determined that attempting to locate the SUBJECT DEVICE could assist in determining the user of the SUBJECT DEVICE and the Thomas_evans977 account. As such, I secured a search warrant (Case No. 4:24-mj-00019-PK) for locational data pertaining to the SUBJECT DEVICE. On February 23, 2024, I executed this search warrant to Verizon for locational data pertaining to the SUBJECT DEVICE. Verizon responded with an automated response stating that beginning on February 24, 2024, at 00:12 Eastern Time, I would receive automated emails approximately every 15 minutes continuing through March 23, 2024, at 23:59 p.m. ET relating to the geographic location of the SUBJECT DEVICE. I confirm that beginning on that date and around that time, I did begin to receive periodic email messages from Verizon containing locational data for the SUBJECT DEVICE.

32. With some *very* limited exceptions, the data received from the ping warrant showed the SUBJECT DEVICE to be in near proximity to the SUBJECT PREMISES. Due to technical limitations, ping data received will usually only place a device within only a general degree of accuracy. For instance, on March 5, 2024, at 9:58:08 PM (UTC), the Latitudinal and Longitudinal coordinates provided were 37.138107 and -113.630379 respectively. Verizon listed the radial accuracy of the ping to be within 402 meters. Listed below is a visual representation of the ping location interpreted by Google in relation to the SUBJECT PREMISES.



33. Based on the scale provided by Google, the SUBJECT PREMISES is well within radial distance of the SUBJECT DEVICE. Again, at the time of this writing, almost all longitudinal and latitudinal data closely approximates the same position as in this example. Further, the SUBJECT PREMISES' distance almost always falls within the ping range provided by each ping data.

34. In reviewing the copious amounts of ping data, I believe the SUBJECT DEVICE is largely stationary and may be being utilized as an Internet source at the SUBJECT PREMISES.

35. As explained below, while the SUBJECT DEVICE appears to be largely stationary, I have noted that there have been some limited instances where the SUBJECT DEVICE pings in locations outside of the SUBJECT PREMISES' ping area. During some of those instances, I have taken steps to observe or document the movements of persons and vehicles to and from the SUBJECT PREMISES.

36. Beginning on March 8, 2024, at approximately 1020 hours, I placed a video-surveillance vehicle in the area of the SUBJECT PREMISES which transmitted video activity around and near the SUBJECT PREMISES. I later reviewed video transmissions date stamped March 9, 2024, at approximately 1625 hours, where I observed a black-colored automobile arrive at the SUBJECT PREMISES. A short time later, I observed two individuals and a leashed canine appear from the area of the front entrance of the SUBJECT PREMISES and enter the black-colored vehicle. At approximately 1628 hours, I observed the vehicle exit the area of the SUBJECT PREMISES. One of the individuals approximately matched the description of GUNTER.

37. In reviewing corresponding ping data, I received information showing that on March 9, 2024, at approximately 1628 hours, the SUBJECT DEVICE was within the approximate radial distance of the SUBJECT PREMISES. At approximately 1644 hours, ping information showed that the SUBJECT DEVICE was pinging approximately six miles or 11 minutes by common vehicle route (based on a Google query between the SUBJECT

PREMISES and the ping location) away from the SUBJECT PREMISES. I have reviewed all the ping data beginning on March 9, 2024, at approximately 1628 hours, and continuing through March 10, 2024, at approximately 0143 hours, and observed ping data showed the SUBJECT DEVICE well outside of the ping area associated with the SUBJECT PREMISES. At approximately 0313 hours on March 10, 2024, I observed that the SUBJECT DEVICE was again pinging from the SUBJECT PREMISES area.[3] I later observed video footage of the SUBJECT PREMISES beginning on March 10, 2024, at approximately 0311 hours and observed a vehicle travel to the area of the SUBJECT PREMISES and come to a stop. A short time later, I observed two individuals and a canine exit the vehicle and walk towards the direction of the SUBJECT PREMISES. Due to diminished lighting, I could not observe detail regarding the vehicle or the individuals.

38. Continuing on March 11, 2024, at approximately 1220 hours, I was in the area of the SUBJECT PREMISES and observed, through video feed and personal observations, a man and woman appear from near the entrance of the SUBJECT PREMISES and mount a motorized scooter parked nearby. At approximately 1224 hours, I observed, through video feed and personal observations, these two individuals exit the area on the motorized scooter. I continued to observe these individuals as they traveled southbound on Dixie Downs Road in St. George, Utah and was able to visually confirm that these two individuals matched the description of GUNTER and Marissa Jean Langnese. I followed the couple to the corner of Dixie Downs Road and West Sunset

[3] Note: Daylight Savings Time occurred at 0200 hours on March 10, 2024.

Avenue. I then observed Marissa Jean Langnese depart from GUNTER and walk to a commercial location, presumably her employer. I then discontinued my visual observations of both individuals.

39. At approximately 1252 hours on March 11, 2024, through video observation, I observed GUNTER return to the SUBJECT PREMISES on a scooter.

40. In reviewing ping data for the period covering the travel of GUNTER and Marissa Langnese to the intersection of Dixie Downs Road and West Sunset Avenue, I observed corresponding changes in ping data. For instance, at approximately 1213 hours on March 11, 2024, I observed that ping data showed the SUBJECT DEVICE within the radial distance of the SUBJECT PREMISES. However, at approximately 1228 hours on March 11, 2024, I showed that the intersection area where I last observed GUNTER and Langnese was within the reported ping area and the SUBJECT PREMISES was no longer within the ping area. A similar ping location was provided at 1243 hours on that same date revealing the intersection to be located within the reported ping area. Again, the SUBJECT PREMISES was not shown as being within the distance of the reported ping area. At approximately 1259 hours on March 11, 2024, ping data shows that the SUBJECT DEVICE was within the ping area of the SUBJECT PREMISES.

41. These corresponding movements of the SUBJECT DEVICE with reported ping data, along with individuals including GUNTER leaving and returning to the SUBJECT PREMISES, suggest the SUBJECT DEVICE is associated with the SUBJECT PREMISES and GUNTER.

42. A DHS summons was issued to Verizon seeking customer call records for the SUBJECT DEVICE. Verizon responded with records showing that between February 24, 2024, and March 5, 2024, 11 calls occurred between call number (435) 359-6851 (call number assigned to SUBJECT DEVICE) and other numbers. I queried all of these numbers in a commonly used law-enforcement database to see associations with the call numbers and individuals. The results of those queries showed that one of the numbers listed was associated with James Alan Gunter and Jade Gunter, who are both referenced earlier and believed to be related to GUNTER. A second number communicating with the call number ((435) 359-6851) was shown to be associated with a Justin Robert Gunter.

43. Based on these observations, and other investigative work explained above, I believe there is probable cause to believe that the SUBJECT DEVICE is routinely located at the SUBJECT PREMISES with GUNTER. Further, probable cause exists to believe GUNTER has access to and/or control of the SUBJECT DEVICE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

44. As described above in Attachment B, this warrant allows law enforcement to search for records that might be found on GUNTER, in the SUBJECT PREMISES, or on the SUBJECT DEVICE in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

45. If a computer or storage medium is found in these locations, person, or device, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media, in particular, computers' internal hard drives, contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

46. As further described in this attachment, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium found on GUNTER, in the SUBJECT PREMISES, and on the SUBJECT DEVICE, because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of

the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such

image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. When an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. A computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

47. Computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macroSD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. During the search of the SUBJECT PREMISES, it is not always possible to search computer equipment and storage devices for data for several reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.

d. Computer users can attempt to conceal data within computer equipment and storage devices through several methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal

data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

48. Computers, routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

49. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

50. The warrant I am applying for would permit law enforcement to compel residents and any other individual present at the SUBJECT PREMISES to unlock any devices requiring biometric access subject to this warrant. This warrant also compels GUNTER to provide biometric data to access the SUBJECT DEVICE or any other devices found at the SUBJECT PREMISES, or on GUNTER's person. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged

in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not

be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of any SUBJECT PREMISES occupants to the fingerprint scanner of the devices found at the SUBJECT PREMISES, or for the SUBJECT DEVICE itself, or on GUNTER's person; (2) hold the devices found at or on the person, device, or locations listed, in front of the face of any SUBJECT PREMISES occupants, to activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES, and on GUNTER's person in front of the face of the SUBJECT PREMISES occupants, as well as GUNTER, to activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement

to compel SUBJECT PREMISES' occupants or any other individual to state or otherwise provide the password or any other means that may be used to unlock or access the devices.

CONCLUSION

51. Based upon the foregoing, there is probable cause to believe that GUNTER collects child pornography—meaning he receives and possesses it. There is probable cause to believe that GUNTER resides at the SUBJECT PREMISES and operates and controls the SUBJECT DEVICE to possess, transport, distribute, and receive child pornography. Therefore, there is probable cause to believe that fruits, evidence and instrumentalities of the Target Offenses, as set forth in Attachment B, will be found on GUNTER, at the SUBJECT PREMISES, and on the SUBJECT DEVICE. I respectfully request that this Court issue a search warrant for the locations and person described in Attachments A-1, A-2, and A-3, authorizing the seizure and search of the items described in Attachment B.

52. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

IVAN J MURRAY
Digitally signed by IVAN J MURRAY
Date: 2024.03.13 15:45:00 -06'00'

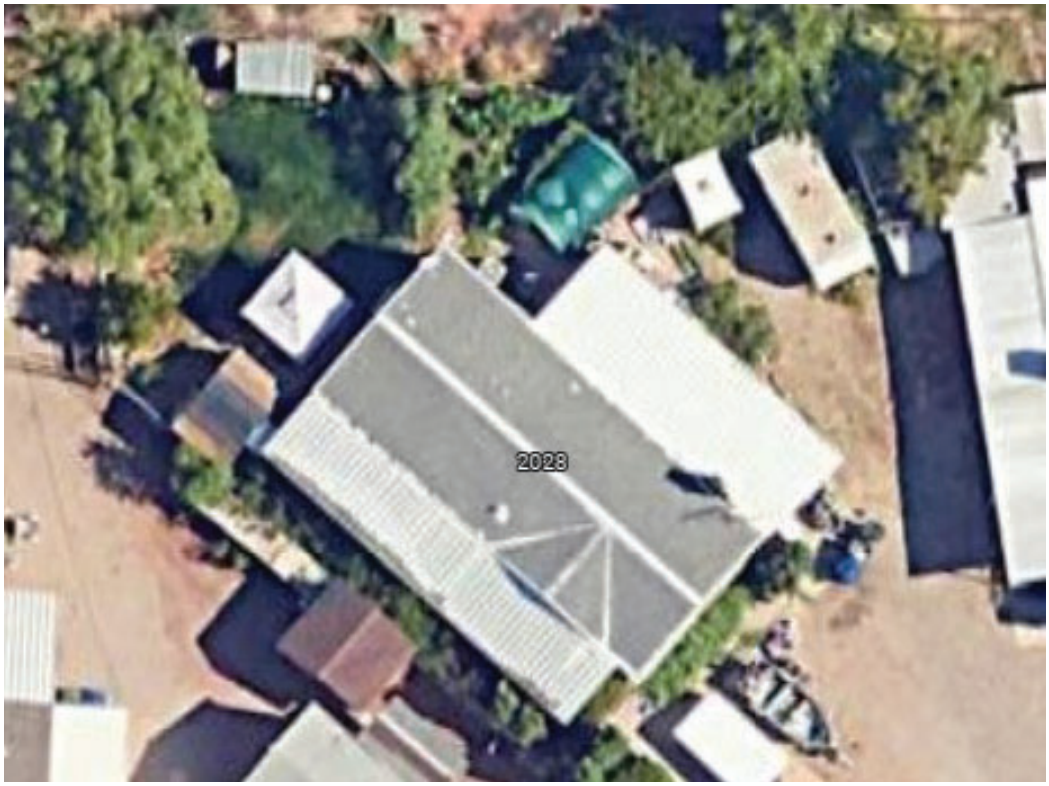
Ivan Murray
Special Agent
Homeland Security Investigations

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1. on March 14, 2024.

PAUL KOHLER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1
PREMISES TO BE SEARCHED

The premises to be searched is located at 2028 W. 1600 N. St. George, UT 84770. The residence is described as a double-wide trailer with white-colored vinyl siding. The numbers "2028" are prominently placed in black-colored numbering on the south-west corner of the structure. The southern end of the structure contains two symmetrical windows to the right of the address numbers.


2028

The premises to be searched includes all garages, outbuildings, sheds, vehicles, and individuals located on the premises at the time of the search.

ATTACHMENT A-2
PERSON AND PROPERTY TO BE SEARCHED

The person to be searched is Johnathan Taylor GUNTER, date of birth [redacted] social security number [redacted]. The property to be searched is any computers, computer equipment, cellular telephones and/or any other electronic media on his person and in the area within his immediate reach, including any personal effects located therein.

ATTACHMENT A-3
DEVICE TO BE SEARCHED

The vehicle to be searched is an Apple iPhone bearing IMEI number 351461186630959.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED AND SEARCHED

The items to be seized include the following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B) (the "Target Offenses"), include the following:

1. Computers or storage media used to commit the Target Offenses described above or that may contain contraband or fruits of the Target Offenses;

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the Target Offenses and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the Target Offenses;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 2028 W. 1600 N. St. George, UT 84770, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

e. Child erotica;

f. Records and information relating to the sexual exploitation of children, including but not limited to correspondence and communications between app users;

g. Records and information showing access to and/or use of Synchronoss account associated with phone numbers (435) 359-6851 and (435) 599-0008;

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

5. During the execution of the search, law enforcement personnel are also specifically authorized to compel all individuals present at the SUBJECT PREMISES, including GUNTER, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the devices found on GUNTER, at the SUBJECT PREMISES, and

b. where the devices are limited to those which can contain and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the device's security features to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any individuals found at the SUBJECT PREMISES, or GUNTER himself, to provide alphanumeric password(s) that may be used to unlock or access the devices, as described in the preceding paragraph, to access or otherwise unlock any device.